CHAPTER

12

REMOTE ACCESS AND VIRTUAL PRIVATE NETWORKS

After reading this chapter and completing the exercises you will be able to:

- Explain how remote access and virtual private network (VPN) services work
- Explain how to implement remote access communications devices and protocols
- Configure remote access services, security, dial-up connectivity, and client access
- Configure VPN services, security, dial-up connectivity, and client access
- Troubleshoot remote access, VPN services, and client connectivity

For millions of computer users who telecommute from home or while traveling, the ability to remotely connect to a network directly affects how they do business. People who telecommute represent one of the fastest growing populations of network users, which is fueling dramatic changes in telecommunications as well as in the capabilities of desktop, laptop, and notebook computers. The client computers used in remote communication connect through a wide range of options, consisting of plain telephone lines, high-speed dedicated lines, cable TV, and satellite communications. Windows 2000 Server comes equipped with Remote Access Server services and virtual private network (VPN) services, which give clients remote access using nearly all conceivable options.

In this chapter you learn how to install, configure, and troubleshoot Windows 2000 Remote Access and VPN server services. You learn to set up security to protect the network that is accessed remotely and to protect the client, and you learn how to set up remote access using simple dial-up modem lines and more complex high-speed communications lines.

How Remote Access Works

There are several ways to remotely access a server on a network. If you use public telephone lines to dial in to your local Internet service provider (ISP), you have already experienced one method of remote access. That method requires that you have a computer with a modem, a computer operating system, and an Internet browser such as Microsoft Internet Explorer. The servers you access may be UNIX, Windows 2000, or other servers that offer a special interface like the Microsoft Internet Information Services (IIS). The files and information that you access are strictly controlled by the capabilities of the interface on the server and the Internet site manager or "Webmaster."

Before widespread use of the Internet, many people accessed their organization's network by dialing into a network workstation running remote access software, such as pcANYWHERE or Carbon Copy. That workstation is left running most of the time so that a single user can dial in to it from a remote computer, such as one at home (see Figure 12-1). The remote computer takes control of the network computer that is left turned on and accesses hosts, servers, or software available through the network. When this method was first used, access was frustrating because modems were slow, and someone might inadvertently turn off the computer connected to the network. Failing to leave the network workstation turned on is still a problem, and there are limitations because the mouse on the network workstation cannot be accessed by the user over the telephone connection.

Another way to set up remote communication is to configure TCP/IP, Telnet (a terminal emulator), and FTP (for file transfer) at the network workstation and leave the workstation turned on. The remote workstation that accesses the network workstation has the same elements configured, and obtains or sends files through FTP. This method also has disadvantages because it is complex to set up, has limited GUI support and enables access to the remote workstation only, and many people fail to set a password because the software is hard to use. Also, there still is the problem that the network workstation may not be left turned on or that a power failure will shut it down.

In the early 1990s Novell improved on remote access technology by introducing the NetWare Access Server (NAS). The original concept of NAS was to make one computer connected to the network act as many workstations in the same unit. For example, a network computer running NAS might contain five modem cards, enabling that number of users to dial in. On that system each user would have a specific portion of the computer to use, including CPU and hard disk space, with the NAS acting like five small computers in one.

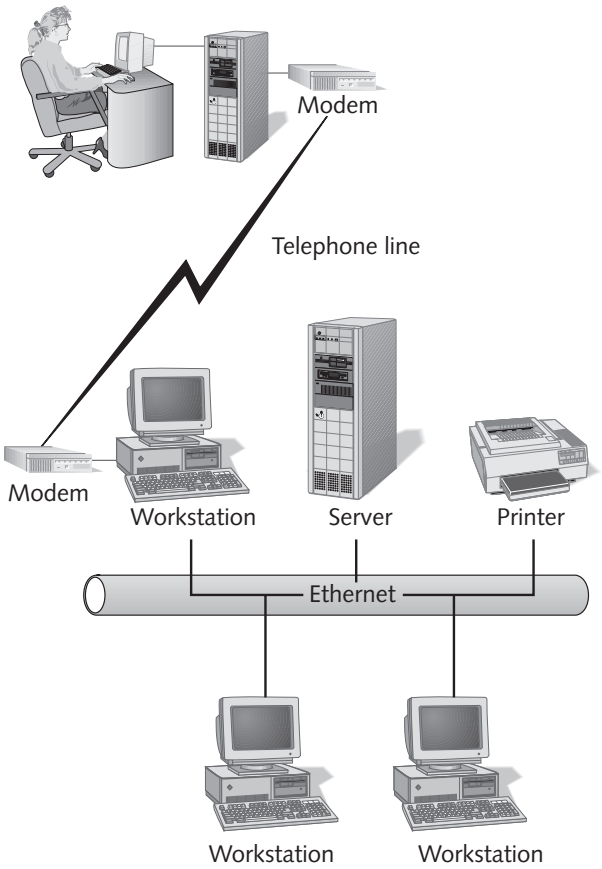

Figure 12-1 Remotely accessing a workstation on a network

Microsoft dramatically improved network access in Windows NT Server—and now in Windows 2000 Server—by enabling a server to double as a remote access server. A computer running Windows 2000 Server can have **Remote Access Services** (**RAS**) installed to turn it into a RAS server capable of handling hundreds of simultaneous connections (see Figure 12-2). The Windows 2000 server performs its normal functions as a server, but serves remote access needs at the same time. A user dials in to the RAS server, providing her or his Windows 2000 Server account name and password, accessing a standalone Windows 2000 server or multiple servers and resources, if the Active Directory is installed. Another way for a client to access the RAS server is through the Internet or an intranet, using specialized tunneling protocols (discussed later in this chapter). If NWLink is set up at the user's workstation and NetWare Client Service is set up in the RAS server, that user also can provide a password to log on to one or more NetWare servers through a Windows 2000 server set up as a RAS server.

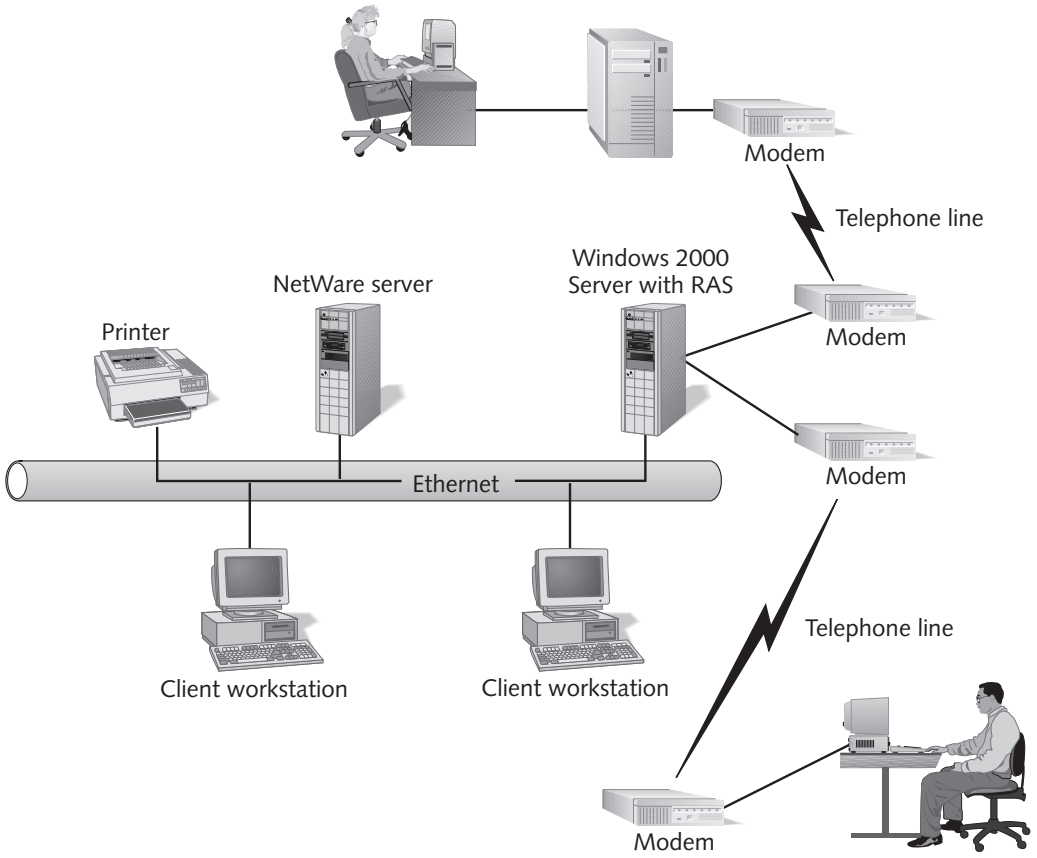

Figure 12-2 Remotely accessing a network through Microsoft RAS

How Virtual Private Networks Work

A **virtual private network** (**VPN**) is an intranet (see Chapters 1 and 3) that is designed for restricted access by specific clients who can be identified in a combination ways: by user account, by IP address, and by subnet address. For example, you might set up a VPN for students at a college so that only authorized students have access to the VPN to look up their academic progress reports and financial information. Another example is to set up a VPN for managers and supervisors in a company to enable them to view confidential sales and accounting information. Many VPNs are accessed remotely by connecting remote networks through routers and by connecting remote VPN clients through dial-up and high-speed communications lines. Some companies are also finding that they can save money on connections by setting up VPNs over the Internet and using World Wide Web communications (see Chapter 13). This is a common use of a Microsoft VPN server in which the server is also configured as a Web server, or connects remote network connections to a Web server. The user accesses the server by starting her or his Web browser and then connecting to the combined Microsoft VPN and Web server over the Internet. Although it is transported over the Internet,

the connection is protected from other Internet traffic, because the VPN/Web server sets up a special communications tunnel within the Internet. An organization can save thousands of dollars in modems and other connection equipment and still enable several hundred remote users to access their network through one or two Internet communications lines.

A Windows 2000 server can be set up as a VPN server by implementing Routing and Remote Access Services and then limiting who can access the server by setting up remote access policies that limit access to only those clients on certain subnets, only those who have certain IP addresses, only those who have certain user accounts, or a combination of these. In the example of the company VPN for managers and supervisors, you might install VPN services on a server that is connected to the subnet 177.28.19, which is used by the company CEO and managers. Access to the VPN server would be limited to only the users on that subnet (users whose IP addresses begin with 177.28.19). Also, the supervisors and some managers, who are scattered throughout different locations and who are on different subnets, can be granted access by authorizing their individual IP addresses, such as 177.28.23.10, 177.28.44.129, and so on. A tunnel can even be set up to a Web server on another subnet, such as 177.28.7. When the CEO, managers, and supervisors are at home or in a remote location, they access the VPN server by connecting through the Internet or through a telecommunications line. You might compare setting up a VPN to creating a private tunnel through a network or the Internet, and telecommunications links for each member client. Clients can access the tunnel from many different locations, but they first must have authorization to enter the tunnel. The particular VPN server that they need to reach is at the end of the tunnel. One network or the Internet can have hundreds of these special tunnels to different locations, and every access to every tunnel is carefully protected (through security protocols) for members only. Figure 12-3 illustrates the architecture of a VPN. In this instance, the Windows 2000 server is also set up to act as a VPN server that authorizes incoming remote clients for access through routers on a network and through two high-speed WAN links: T-carrier and frame relay. A **T-carrier** link is a WAN link that supports different levels of high-speed computing through lines that supply multiple communications channels. The most common versions are T-1 for communications up to 1.544 Mbps, and T-3 for communications up to 44.736 Mbps. **Frame relay** is a high-speed WAN communications technology that uses switched channels for communications that range from 56 Kbps to 45 Mbps. The combined VPN server acts like a network guardian for those who access the network remotely.

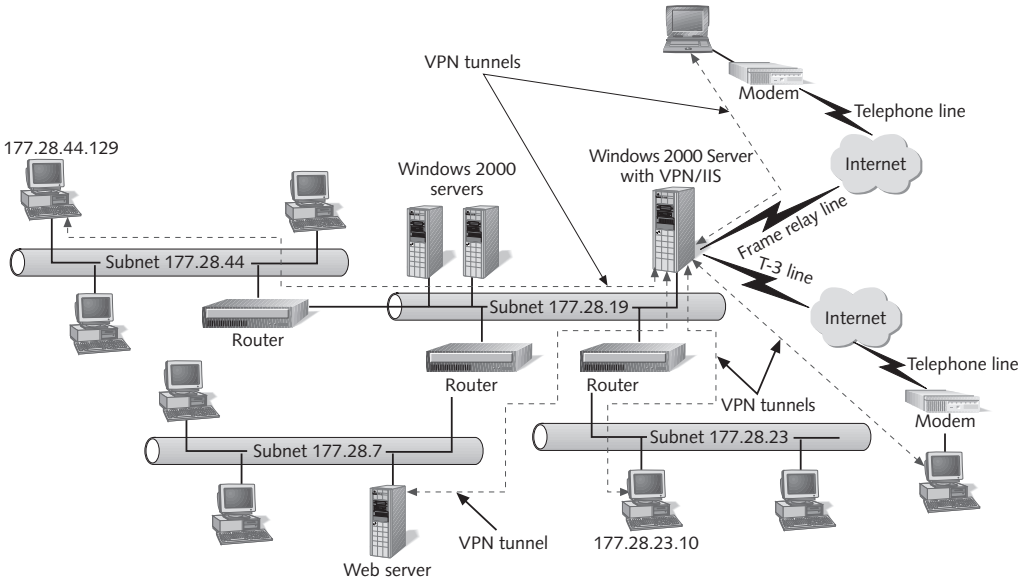

Figure 12-3 VPN network architecture

Using Microsoft Remote Access Services

A Windows 2000 server that is also a RAS server offers secure, flexible remote access into that server and to other Windows 2000, Windows NT, and NetWare servers on a network. A computer with one or more modems and the Windows 2000 Server or Windows 2000 Professional operating system can be set up for RAS, because RAS is included with the operating system. Windows 2000 Professional is a limited RAS server because it can handle only one caller at a time. Windows 2000 Server enables up to 256 dial-in remote callers and a nearly unlimited number (depending on the hardware) of Internet-based clients to connect at the same time. A RAS server offers remote connectivity to the following client operating systems:

- MS-DOS
- Windows 3.1 and 3.11 (Windows for Workgroups)
- Windows NT (all versions)
- Windows 95
- Windows 98
- Windows 2000 Server and Professional

Not only is it designed to work with many kinds of clients, but a RAS server also supports the following types of connections:

- Asynchronous modems (such as the modem you may already use in your PC)
- Synchronous modems through an access server
- Null modem communications
- Regular dial-up telephone lines
- Leased telecommunication lines, such as T-carrier
- ISDN lines (and digital modems)
- X.25 lines
- DSL lines
- Frame relay lines

Integrated Services Digital Network (**ISDN**) is a standard for delivering data services over specialized digital telephone lines using 64 Kbps channels. The channels are combined to offer different types of services, for example, an ISDN basic rate interface consists of three channels. Two are 64 Kbps channels for data, voice, and graphics transmissions. The third channel is a 16 Kbps channel used for communications signaling. Many United States telecommunications companies offer ISDN, which is often used for industrial-strength Internet connectivity. **X.25** is an older WAN communications method originally used to transmit data over telecommunications lines at speeds up to 64 Kbps, but upgraded in 1992 to provide speeds up to 2.048 Mbps. X.25 is more commonly used in Europe and other countries than in the United States or Canada.

One of the most common ways to connect is by using asynchronous modems and dial-up telephone lines, which in many areas offer 56 Kbps connectivity through regular modems. In some areas, telecommunications companies offer **digital subscriber line** (**DSL**) technology over regular telephone lines that enable upstream (sending from the client) communications that are as fast as 2.048 Mbps and downstream (receiving at the client) communications at up to 60 Mbps. As you plan what services to use, purchase modems and communications adapters (such as those for ISDN, DSL, and X.25) listed in the hardware compatibility list (HCL, see Chapter 2).

Microsoft RAS provides support for the standardized modem driver, **Universal Modem Driver**, used by recently developed modems. It also contains support for the **Telephone Application Programming Interface** (**TAPI**). TAPI is an interface for line device functions, such as automatic dialing, call holding, call receiving, call hang-up, and call forwarding. **Line devices** are communications equipment such as modems, ISDN adapters, X.25 adapters, and fax cards that directly connect to a telecommunications line.

Besides supporting different types of modems and communications equipment, Windows 2000 RAS is compatible with the following network transport and remote communications protocols:

- NetBEUI
- TCP/IP
- NWLink
- PPP
- PPTP
- L2TP

Implementing Remote Communications Devices

Improvements in remote access have involved dramatic improvements in remote communications devices such as modems. Modems are a key piece in making remote access possible and worthwhile. The term **modem** is a shortened version of the full name, modulator/demodulator. This device converts a computer's outgoing digital signal to an analog signal that can be transmitted over a telephone line. It also converts the incoming analog signal to a digital signal that the computer can understand. A modem is attached to a computer in one of two ways: internally or externally. An internal modem is installed inside the computer, using an empty expansion slot on the main board. An external modem is a separate device that connects to a serial or USB port on the computer. An external modem is attached by using a cable that is designed for modem communications and that matches the serial port or USB connector on the computer. The most commonly used type of modem is asynchronous, which means that each unit of information is communicated using a special signal or data bit to show the start and end of a unit during transmission. Synchronous modems are less commonly used and employ a clocking technique to indicate the start and end of a communications unit.

The modem data transfer rate is measured in **bits per second** (**bps**). Dial-up telephone line modems are currently capable of up to 56 Kbps rates, and are soon expected to reach over 100 Kbps. Cable TV modems transmit at a much higher rate, depending on the modem and the cable TV company. For example, one vendor's modem transmits at up to 30 Mbps for upstream (sending) communications and at up to 15 Mbps for downstream (receiving).

Cable TV RAS communications are not recommended at this writing because there can be security problems that enable other cable subscribers to intercept your communications.

When a computer is connected to a modem, the data transfer speed is the **data terminal equipment** (**DTE**), communications rate. A workstation client and the RAS server are both examples of DTE because they prepare data to be transmitted. The modem is called the **data communications equipment** (**DCE**), and its speed is the DCE communications rate. The computer's port setup for the modem (DTE rate) should be the same or higher than the DCE rate of the modem. For example, if you have a 56 Kbps modem, select a maximum speed of 57600 (the closest setting) in Windows 2000 Server when you configure the computer for that modem. (You can view how a modem and its computer port are set up in Hands-on Project 12-1).

Sometimes modems will not communicate because of how they are set up. For example, an older 14.4 Kbps modem on a client will not be able to establish communications with a newer 56 Kbps modem, if the 56 Kbps modem is not set up to negotiate down to a slower speed. Also, when telephone lines are very noisy, some modems attempt to step down to a slower speed for data compression. If one of the communicating modems does not have data compression capability or cannot automatically step down to a slower speed, they may not be able to establish a link-up. Keep these cautions in mind when you set up network modems and work with users to solve modem communication problems.

ISDN requires using a **terminal adapter** (**TA**) to connect a computer to an ISDN line. A TA also is called a digital modem, even though it is not truly a modulator/demodulator, because it uses digital instead of analog technology. ISDN digital TAs are available for about the same cost as a high-quality asynchronous modem, but with higher data transfer capabilities, such as 128 Kbps or faster. If you connect using X.25 or DSL, then you will need a specialized X.25 or DSL adapter to install in the computer. (T-carrier and frame relay are typically connected by using an access server or a router that forwards communications to the Windows RAS or VPN server.)

Use the Add/Remove Hardware Wizard to install regular telephone modems, DSL adapters, ISDN TAs, or X.25 adapters. Also, use the Network and Dial-up Connections tool to create a specialized connection for each type of device (see the section titled "Configuring a Dial-up Connection for a RAS Server").

One advantage when using ISDN is that it is possible to link multiple lines or communications channels as though they were one, for example linking two 64 Kbps channels into one 128 Kbps link, called an **aggregate link**. Windows 2000 Server can configure aggregate links by using Multilink, which is described later in this chapter.

If you need to provide remote access by setting up more than two modems or by offering several different access options, such as a combination of regular analog modems, ISDN, and X.25 lines, consider using an access server. An **access server** is a device that connects directly to a network at one end and that offers combinations of communications options for connecting to outside telecommunications lines. An access server can be equipped with one or more TAs, X.25 adapters, and modems. For example, one access server might contain 16 modem connections (sometimes called a modem bank), two ISDN connections through the appropriate types of adapters, and one T-1 connection. Some modular access servers can have nearly 70 modems and are equipped with redundant power supplies for fault tolerance. Further, many access servers include specialized software to work with a Windows 2000 server over a network to provide connectivity for RAS clients and for Web server clients. Figure 12-4 illustrates an access server.

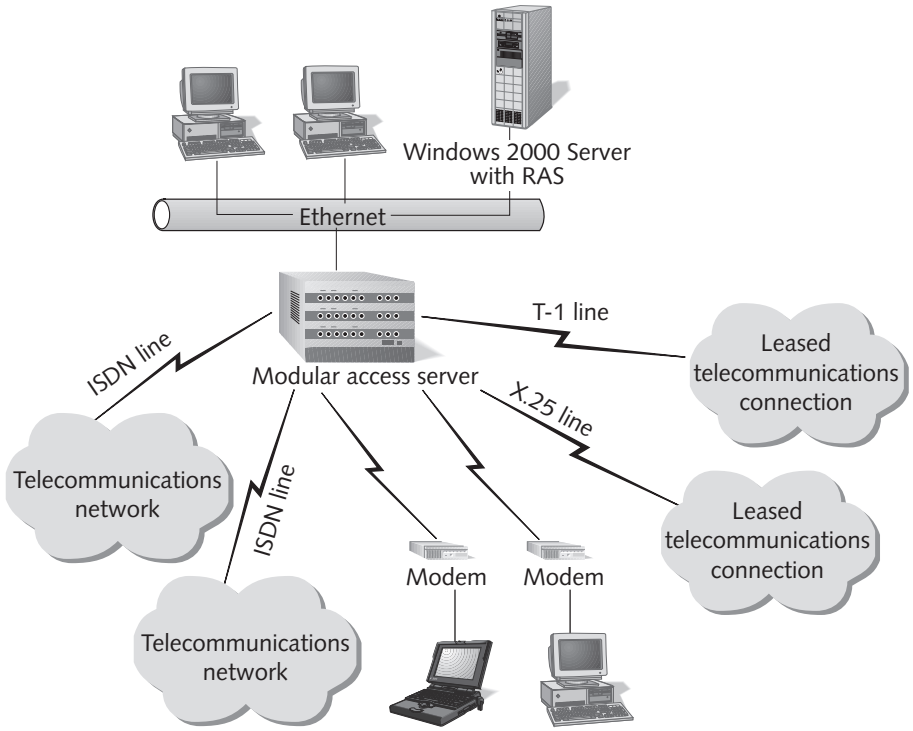

Figure 12-4 Using an access server

Implementing Remote Access Protocols

Two protocols are used most frequently in remote communications: SLIP and PPP. **Serial Line Internet Protocol** (**SLIP**) was originally designed for UNIX environments for point-to-point communications among computers, servers, and hosts using TCP/IP. SLIP is an older remote communications protocol with more overhead (larger packet header and more network traffic) than PPP. Compressed Serial Line Internet Protocol (CSLIP) is a newer version of SLIP that compresses header information in each packet sent across a remote link. CSLIP, now usually referred to as SLIP, reduces the overhead of a connection so that it is less than that of PPP, by decreasing the header size and thus increasing the speed of communications. However, the header still must be decompressed at the receiving end. The original SLIP and the newer SLIP (CSLIP) are limited in that they do not support network connection authentication to prevent someone from intercepting a communication. They also do not support automatic negotiation of the network connection through multiple network connection layers at the same time. Another disadvantage of both versions of SLIP is that they are intended only for asynchronous communications, such as through a modem-to-modem type of connection.

Point-to-Point Protocol (**PPP**) is used more commonly than either version of SLIP for remote communications because it has lower overhead and more capability. PPP supports more network protocols, such as IPX/SPX, NetBEUI, and TCP/IP. It can automatically

negotiate communications with several network communications layers at once, and it supports connection authentication. PPP is supplemented by the newer **Point-to-Point Tunneling Protocol** (**PPTP**), which enables remote communications to RAS and a VPN through the Internet or an intranet. Through PPTP, a company manager can access a report housed on that company's in-house intranet by dialing in to the Internet from a remote location. Microsoft VPN networks also use **Layer Two Tunneling Protocol** (**L2TP**), which works similarly to PPTP. Both protocols encapsulate PPP and create special tunnels within a network or over the Internet that reflect intranets and VPNs. Unlike PPTP, L2TP uses an additional network communications standard, called Layer Two Forwarding, that enables forwarding on the basis of MAC addressing (device address, see Chapter 3) in addition to IP addressing. PPP, PPTP, and L2TP all support the security measures described later in this chapter.

As you think about protocols encapsulating protocols, consider the process of shipping a computer in the mail. The computer is packaged in protective styrofoam, and then sealed in a box. In the same way, TCP/IP (and other network protocols, such as NWLink) is encapsulated in PPP to be shipped over a remote network, and then PPP is encapsulated in PPTP or L2TP for shipment over the Internet, an intranet, or a VPN.

PPP and PPTP both support synchronous and asynchronous communications, enabling connectivity through modems, dial-up and high-speed leased telecommunication lines, DSL lines, ISDN, and X.25 lines. On the client side, PPP is available in Windows 95, Windows 98, all versions of Windows NT, and all versions of Windows 2000. *When a Windows 2000 server is also configured as a RAS server, supports PPP and its associated protocols, but not SLIP.* PPP configuration is well suited on networks in which users perform remote access through computers running Windows 95, 98, NT, or 2000. Table 12-1 compares SLIP to PPP.

Windows NT Server 4.0 supports either SLIP or PPP when configured as a RAS server. If you convert Windows NT Server 4.0, set up with RAS and using SLIP, to Windows 2000 Server, plan to convert the RAS implementation and all RAS clients to use PPP.

Table 12-1 SLIP and PPP Compared

Feature	SLIP	PPP
Network protocol support	TCP/IP	TCP/IP, IPX/SPX, and NetBEUI
Asynchronous communications support	Yes	Yes
Synchronous communications support	No	Yes
Simultaneous network configuration negotiation and automatic connection with multiple levels of the OSI model between the communicating nodes	No	Yes
Support for connection authentication to guard against eavesdroppers	No	Yes

CONFIGURING RAS

There are several essential steps to configuring RAS communications on a Windows 2000 Server network:

- Configuring a Microsoft 2000 server as a network's RAS server, including configuring the right protocols to provide RAS access through dial-up connectivity
- Configuring a DHCP Relay Agent for TCP/IP communications
- Configuring RAS security
- Configuring a dial-up and remote connection
- Configuring RAS on client workstations

Configuring a RAS Server

There are two components to making a Windows 2000 server double as a RAS server. You already have learned the first component, which is to implement a way to connect multiple modems to a network. On a very small network you may need to install only one or two modems directly into an existing networked computer running Microsoft 2000 Server. For a larger network, you can install an access server with enough modems, ISDN, and other types of connections for the type of communications required by users.

Choose an access server that is designed to be compatible with Microsoft 2000 Server. A compatible access server will include software and drivers that can be used to coordinate communications between the Windows 2000 server and the access server, including IP routing capabilities.

The second component is to install the software needed to turn the Windows 2000 server into a RAS server. (As for most other administrative functions, you must be logged on as Administrator or with Administrator privileges.) You install RAS using the Routing and Remote Access tool, which is opened from the Administrative Tools menu or as an MMC snap-in. For example, to start the tool from the Administrative Tools menu, click Start, point to Programs, point to Administrative Tools, and click Routing and Remote Access. After the tool is started:

1. Click Routing and Remote Access in the tree, if it is not already selected, click the Action menu, and click Add Server.
2. The Add Server dialog box enables you to install routing and RAS capabilities on the local server or on another Windows 2000 server connected to the network or in the domain. Also, there is a Browse button that enables you to search for another server on which to install the services. For example, click *This computer* to install routing and RAS on the local server, and then click OK.

3. Under the tree, right-click the computer and click Configure and Enable Routing and Remote Access (see Figure 12-5).

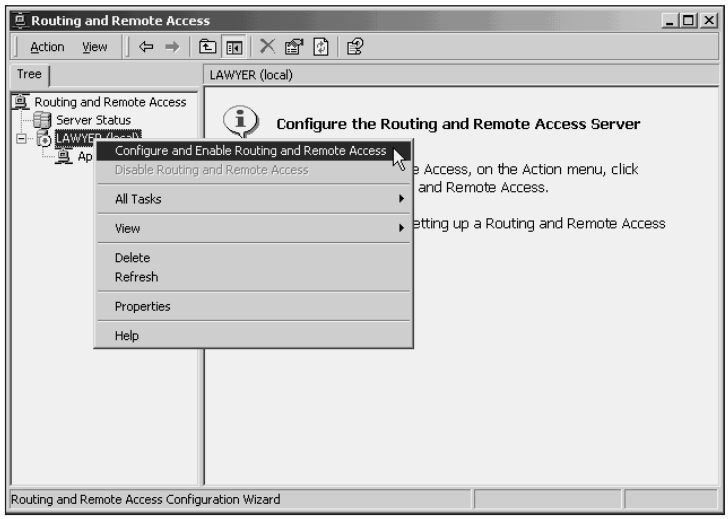

Figure 12-5 Configuring routing and RAS

4. Click Next after the Routing and Remote Access Server Setup Wizard starts.
5. There are five options (see Figure 12-6 and Table 12-2) from which to select. Click *Remote access server* to make this a RAS server, and then click Next.
6. If a screen displays asking you to choose between creating a basic or advanced remote access server, select set up an advanced remote access server.

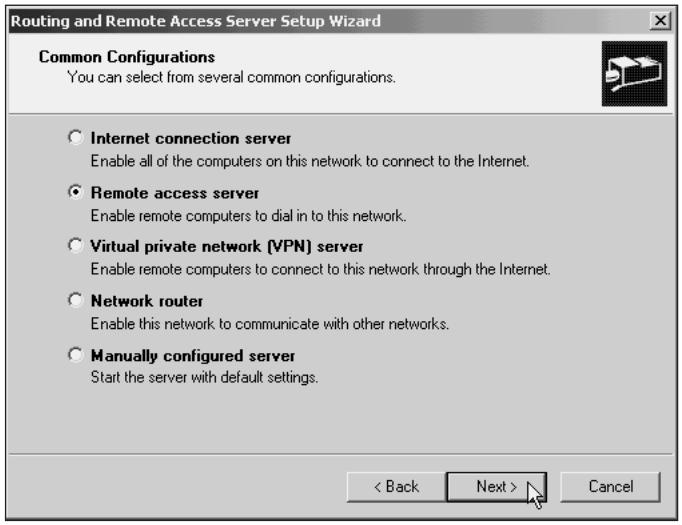

Figure 12-6 Selecting the option to install RAS

Table 12-2 Routing and Remote Access Options

Option	Description
Internet connection server	Use this option so that networked computers in addition to the server can connect to the Internet, which is especially useful in a small office environment in which all users need Internet access, but there is only one dial-up, ISDN, or other outside line to an ISP.
Remote access server	Use this option to set up remote access services to the network through the Windows 2000 server.
Virtual private network (VPN) server	Use this option when you have an intranet (VPN) that you want users to be able to access through a remote connection or the Internet.
Network router	Use this option to have Windows 2000 Server function as a router on the network—directing traffic to other networks or subnetworks.
Manually configure the server	Use this option when you want to customize the routing and remote access capabilities.

7. The protocols that are already installed on the server are displayed. Click Yes to use all of the protocols listed, or click No if you need to add protocols to the list for support through RAS. Click Next. (If you clicked No, then click Next and click Finish on the next screen to end the Wizard, install the additional protocols, and restart the Wizard.)
8. If you clicked Yes and AppleTalk is among the supported protocols, the Wizard displays a dialog box to enable AppleTalk clients to access the RAS server through the Guest account.

If you enable AppleTalk access, you cannot set a password for the Guest account. This means you should carefully check what resources are available through the Guest account, because they can be accessed by anyone, including intruders. If the Macintosh clients support IP (such as MAC OS 8.5 and higher), consider using IP instead of AppleTalk to access the RAS server.

9. If TCP/IP is one of the installed protocols, then the Wizard displays a dialog box with two options (see Figure 12-7), to use DHCP to automatically assign IP addresses for clients who access the network through RAS or for you to manually specify a range of IP addresses. If you choose to specify a range of addresses, a specialized dialog box is displayed in which to enter the range; make sure that none of the addresses in the range is already in use by any network client. Also, if you have Internet access and use an ISP, consult your ISP about what range is acceptable and will not interfere with other Internet sites. Click Next after you make your selection.

Figure 12-7 IP address assignment options

10. In the Managing Multiple and Remote Access Servers dialog box, you have the option to make this or another RAS server a **Remote Authentication Dial-in User Service** (**RADIUS**) server. A RADIUS server is used when you plan to set up two or more RAS servers and want to standardize access policies and authentication. If you have only a standalone server or plan to have only one RAS server, click No and then click Next. If you plan to set up additional RAS servers, for example in a domain, click Yes. Clicking Yes and then Next displays another dialog box on which to specify one RADIUS server to coordinate authentication and to keep track of remote dial-in statistics for all RAS servers. You can also specify an alternate RADIUS server as a backup and a password to enable the RAS server to access the RADIUS server. Further, if you click Yes, you should also later install the **Internet Authentication Service** (**IAS**) through the Add/Remove Programs utility. IAS enables you to establish security (discussed later in this chapter) for RAS dial-in access.
11. Click Finish. (If you configured to use DHCP for IP address assignment, also click OK in the information message that you must configure the RAS server as a DHCP Relay Agent.)

If you selected to automatically assign IP addresses and are using DHCP, configure the DHCP Relay Agent so that it contains the IP address of the RAS server. A **DHCP Relay Agent** broadcasts IP configuration information between the DHCP server and the client acquiring an address, when they are on different networks.

Try Hands-on Project 12-2 to set up a RAS server.

After the RAS server is set up, you can further configure it from the Routing and Remote Access tool by right-clicking the RAS server in the tree and clicking Properties (see Figure 12-8). For

example, the Properties dialog box has a tab for each protocol that you have configured, and each protocol's tab is used to enable or disable that protocol for remote access. Also, the IP tab is used to specify how IP addresses are assigned (DHCP or a manually specified range). The IPX tab is used to specify how IPX network numbers are assigned (for access to older NetWare servers), and the NetBEUI tab is used to specify whether NetBEUI use applies only to the RAS server or to the entire network. Also, there is a General tab on which you can configure Windows 2000 Server to function as a router for the LAN or for the LAN and for dial-in client connections. The Security tab is used to configure security and authentication methods, which you will explore later in this chapter. The PPP tab is used to configure PPP options, such as aggregating ISDN connections (also discussed later in this chapter). Last, there is a tab to configure event logging, such as access errors and warnings or errors using the PPP protocol.

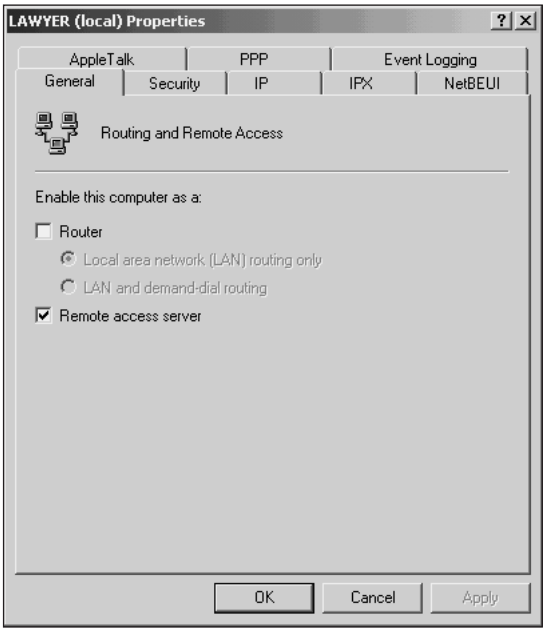

Figure 12-8 RAS server properties

Configuring a DHCP Agent

When a RAS server is configured so that the IP addresses of RAS dial-in clients are obtained automatically, then the RAS server must be designated as a DHCP Relay Agent. Use the following steps to configure a DHCP Relay Agent:

1. Open the Routing and Remote Access tool.
2. Double-click the RAS server in the tree.
3. Click IP Routing in the tree.
4. Right-click DHCP Relay Agent in the IP Routing pane, and click Properties.

5. Enter the IP address of the RAS server and click Add.
6. Click OK.

You can further configure the DHCP Relay Agent by specifying the maximum number of routers, called the hop count, that an IP configuration broadcast can pass through between the client, RAS server, and DHCP server. Click DHCP Relay Agent under the tree, right-click the interface, such as Internal, and then click Properties. Make sure that the Relay DHCP packets box is checked, and then specify the *Hop-count threshold*. For example, consider a situation in which each client must go through one router to reach the RAS server, and the RAS server must go through one router to reach the DHCP server. In this example, the threshold should be set at 2 or 3 if the server is configured as a router (try Hands-on Project 12-3).

Configuring Multilink and Bandwidth Allocation Protocol

A RAS server can be configured to support **Multilink** (also called **Multilink PPP**). Multilink is used to combine or aggregate two or more communications channels so they appear as one large channel. For example, Multilink can combine two 64 Kbps ISDN channels and one 16 Kbps signaling channel in the *basic rate interface* service to appear as one 144 Kbps channel; or, multiple 64 Kbps *primary rate interface* channels and one 64 Kbps signaling channel are aggregated into 1.536 Mbps. Another example is combining two 56 Kbps modems into an aggregate speed of 112 Kbps. The limitation of using Multilink is that it must be implemented in the client as well as in the server, so that the client can take full advantage of the aggregated links. Thus if you use Multilink to aggregate two 56 Kbps modems for one 112 Kbps link at the server, the client, such as Windows 2000 Professional, must have a communications link set up using Multilink to aggregate two 56 Kbps modems.

Multilink can be used with **Bandwidth Allocation Protocol** (**BAP**) to ensure that a client's connection has enough speed or bandwidth for a particular application. BAP helps ensure that the amount of bandwidth increases to the maximum for the aggregated channels as needed, and reciprocally contracts as the need becomes less. For example, consider a connection in which the remote client begins by accessing a relatively low-bandwidth application such as e-mail over an aggregated link of two 56 Kbps modems. BAP might determine that only 56 Kbps is needed for the application. However, when the client accesses a voice and video presentation in a multimedia application, such as a chemistry lesson or a movie clip, BAP can increase the bandwidth to the full aggregated speed of 112 Kbps by adding the line to the second modem for the duration of the multimedia presentation. BAP matches bandwidth utilization to the need, so that unused bandwidth can be given to another client whenever possible. Besides adding a line for use by a client, BAP can hang up a line so that another client can use it.

To configure Multilink and BAP, right-click the RAS server in the Routing and Remote Access tool, click Properties, and then click the PPP tab (see Figure 12-9). Check the *Multilink connections* option to enable Multilink, and check *Dynamic bandwidth control using BAP or BACP* to use BAP or BACP. (**BACP** is the **Bandwidth Allocation Control Protocol**, which selects a preferred client when two or more clients vie for the same bandwidth.)

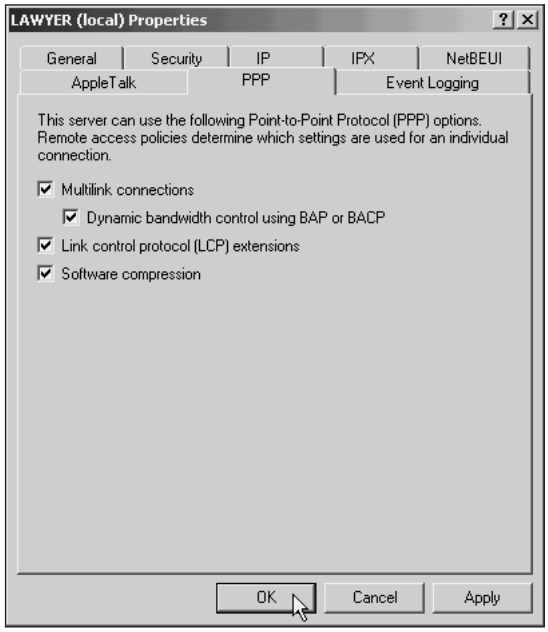

Figure 12-9 Configuring Multilink and BAP

The option to use Link control protocol (LCP) extensions should also be checked when you want to use callback security (discussed later in this chapter). Also, check the *Software compression* option to compress data over a remote link for faster transport. This option enables the use of the Microsoft Point-to-Point Compression Protocol (try Hands-on Project 12-4).

Configuring Security and RAS Options Through a RAS Policy and Profile

When a user accesses a RAS server through his or her account, that access is protected by the account access security that already applies, for example through a group policy or the default domain policy. Thus, if account lockout is set up in a group policy, the same account lockout settings apply when a RAS user enters her or his account name and password. Besides the security policies already in place, you can set up RAS security through several other techniques, which include creating user account dial-in security, setting remote access group policies, and establishing security through protocols.

The first step to take is to set up dial-in security at the user account, which enables you to employ callback security. (Recall from Chapter 8 that callback security entails having the RAS server call back the workstation that is requesting access.) This security is set on each user's Windows 2000 server or domain account. For example, the remote workstation client calls into the RAS server to access a particular Windows 2000 server user account. With callback security set up, the server calls back the remote computer to verify its telephone number,

in order to discourage a hacker from trying to access the server. The callback options available in Windows 2000 Server are the following:

- *No Callback*, which means the server allows access on the first call attempt
- *Set By Caller*, so that the number used for the callback is provided by the remote computer
- *Always Callback to*, so the number to call back is already permanently entered into Windows 2000

To set up callback security on a particular user account, double-click the account and set the dial-in security in the account's properties (try Hands-on Project 12-5). For example, if the Active Directory is installed:

1. Open the Active Directory Users and Computers tool.
2. If necessary to display the objects under it, double-click the domain in which the account resides, and then double-click the container holding the account, such as Users.
3. Right-click the account on which you want to set up dial-in security, and click Properties.
4. Depending on how Windows 2000 automatically adjusts to your screen's resolution and capabilities, the next screen shows all user Properties tabs or displays double arrows from which to view the tabs (see Figure 12-10). Access the Dial-in tab by clicking it in the display of tabs or by using the double arrows and then clicking to open the tab.

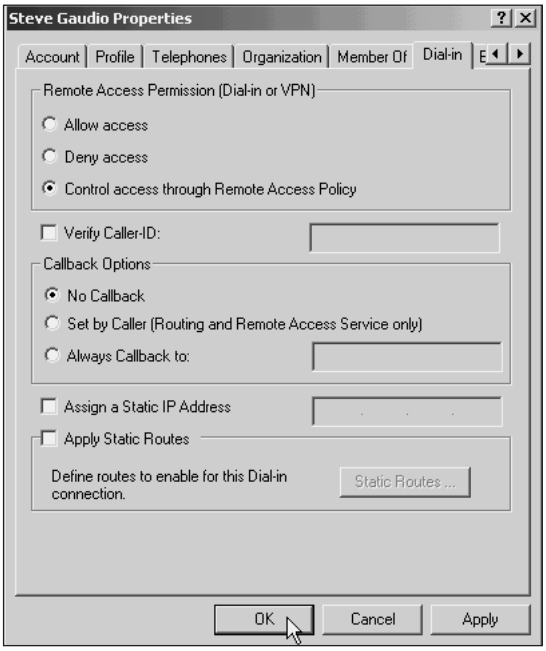

Figure 12-10 Configuring dial-in security for a user account

5. Click the Allow access radio button or click Control access through Remote Access Policy (remote access policies are described later in this section).
6. Click Verify Caller-ID and provide the user's telephone number, if that user and your organization have Caller ID and the user will always use the same number to dial in remotely.
7. Select the callback option (enter a telephone number to call back if you select *Always Callback to*).
8. Select whether to define a static IP address that will always apply to anyone who dials in remotely to that account and whether to use static routing (or leave the boxes blank to enable DHCP and IAS to determine an IP address and routing).
9. Click OK.

Some Dial-in parameters are deactivated (grayed-out) if you are operating in mixed mode instead of native mode (see Chapter 9). These parameters include Control Access through Remote Access Policy, Verify Caller-ID, Assign a Static IP Address, and Apply Static Routes.

When you decide to set up remote access policies for dial-in RAS or VPN servers (see the section "Configuring a VPN Server"), first install IAS (Internet Authentication Service) to enable you to centrally manage one or more RAS servers. IAS is installed by following these steps:

1. Open the Control Panel and double-click Add/Remove Programs.
2. Click Add/Remove Windows Components. If the Windows Components Wizard dialog box is not automatically started, click the Components button to start it.
3. When the Windows Components Wizard starts, scroll to find Networking Services and then double-click that option.
4. Make sure the box for Internet Authentication Service is checked (along with any other services you want to add), and click OK.
5. Click Next.
6. Click Finish.
7. Close the Add/Remove Programs window and the Control Panels.

If you have only one RAS or VPN server, you can set the remote access policies on a single server by using the Routing and Remote Access Tool, double-clicking the server, and double-clicking *Allow access if dial-in permission is enabled*. Then complete the parameters, which are the same as those described next for IAS member servers coordinated by RADIUS.

After IAS is installed, add participating RAS and VPN servers by opening the Internet Authentication Service, which is accessed by clicking Start, pointing to Programs, pointing to Administrative Tools, and clicking Internet Authentication Service. To add a server, right-click Clients under Internet Authentication Service in the tree and click New Client. Provide the name of the client server, and click Next. Provide the IP address of the server, select RADIUS Standard for the Client-Vendor, provide a secret RADIUS password in the

Shared secret box, confirm the password, and click Finish. Use the Remote Access Policies object in the tree to configure several types of security that include (but are not limited to):

- Granting dial-in access, if dial-in access is also granted on a user's account
- Specifying dial-in constraints, such as the hours and days when RAS can be accessed
- Setting IP address assignment rules
- Setting authentication
- Setting encryption
- Allowing Multilink connections

To begin configuring security, click Remote Access Policies in the tree and double-click *Allow access if dial-in permission is enabled*, to display the dialog box in Figure 12-11. The name of the policy is displayed in the Policy name box, enabling you to create one or more policies with unique names. By default the name is "Allow access if dial-in permission is enabled." Below the Policy name box is another box that enables you to set the time of day and day of the week restrictions on when a user can access RAS servers. To change these settings, double-click the default that is already highlighted, click the Grant or Deny radio buttons, use your pointing device to mark the desired times and days, and click OK. Click the Add button to set up additional access attributes, such as a particular telephone number that must be used by an account, or to specify that the user must belong to a particular predefined group, such as RAS Users. Finally, click the Grant remote access permission radio button to enable users to access the RAS and VPN servers on the basis of conditions you set up in the *Specify conditions to match* box (try Hands-on Project 12-6).

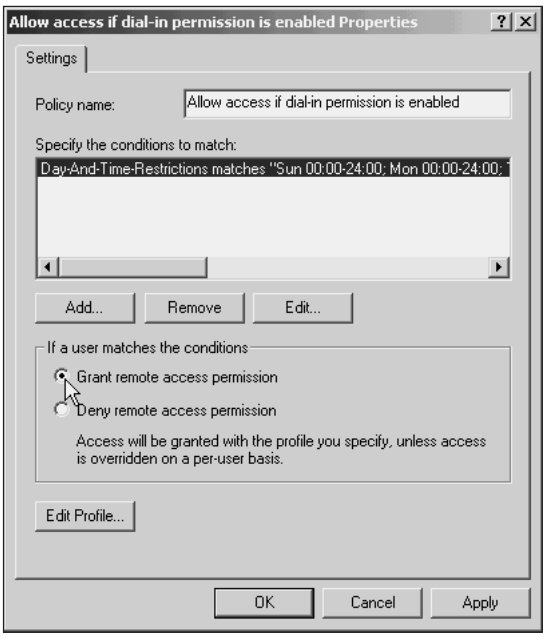

Figure 12-11 Granting remote access as a RAS policy

One way to manage users' access to RAS and VPN servers is to set up only specific user accounts to grant dial-in access or to control access through the remote access policies (see Figure 12-10). If you control access through the remote access policies, consider fine-tuning the management of user account access by creating groups. For example, create a universal or domain local group that has access to one or more RAS or VPN servers, and create a global group of the user accounts that you want to have the access. Make the global group a member of the universal or domain local group. Next, open the Remote Access Policies object under the RAS or VPN server, click the Add button (see Figure 12-11), double-click Windows-Groups, click Add, double-click the universal or domain local group you created, click OK, and click OK twice.

To configure the profile and security associated with the remote access policies, click the Edit Profile button to view the dialog box shown in Figure 12-12. The options for each tab are summarized in Table 12-3. The tabs that particularly affect security are the Authentication and the Encryption tabs. The Authentication tab enables you to set up security through protocols that work with PPP, which are:

- **Extensible Authentication Protocol** (**EAP**): EAP is used for clients who access RAS through special devices such as smart cards, token cards, and others that use certificate authentication. If you click this option, then Certificate Services should be installed so that you can configure them for a particular device or certificate type. Certificate Services is installed as a Windows component by using the Control Panel Add/Remove Programs tool.
- **Challenge Handshake Authentication Protocol** (**CHAP**): CHAP requires encrypted authentication between the server and the client, but uses a generic form of password encryption, which enables UNIX computers and other non-Microsoft operating systems to connect to a RAS server.
- **CHAP with Microsoft extensions** (**MS-CHAP**): MS-CHAP and MS-CHAP v2 are set as the defaults when you install a RAS server, which means that clients must use MS-CHAP with PPP. MS-CHAP is a version of CHAP that uses a challenge-and-response form of authentication along with encryption. Windows 95, 98, NT, and 2000 support MS-CHAP.
- **CHAP with Microsoft extensions version 2** (**MS-CHAP v2**): Developed especially for VPNs, MS-CHAP v2 provides better authentication than MS-CHAP, because it requires the server and the client to authenticate mutually. It also provides more sophisticated encryption by using a different encryption key for receiving than for sending. Windows 2000 clients support MS-CHAP v2 and clients such as Windows 95 and Windows 98 can be updated to support this protocol. VPNs attempt to use MS-CHAP v2 with a client and then use MS-CHAP if the client does not support version 2.
- **Password Authentication Protocol** (**PAP**): PAP can perform authentication, but does not require it, which means that operating systems without password encryption capabilities, such as MS-DOS, are able to connect to RAS.

- **Shiva Password Authentication Protocol** (**SPAP**): SPAP provides PAP services for remote access clients, network equipment, and network management software manufactured by the Shiva Corporation, which is owned by Intel Corporation.

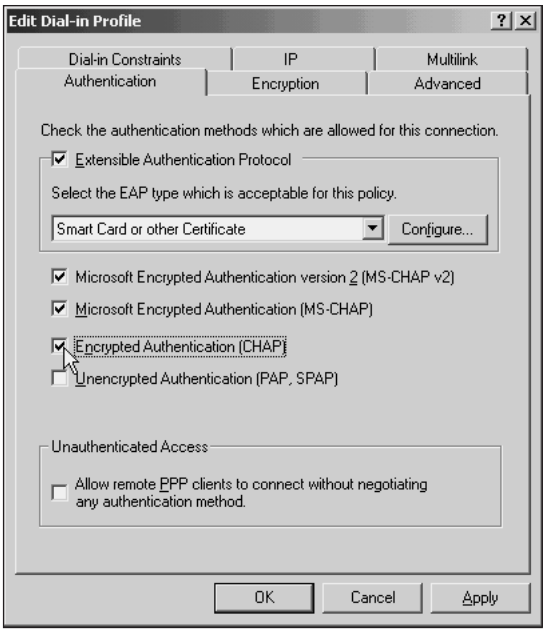

Figure 12-12 Configuring authentication

You can use one or a combination of these authentication protocols, and if you use a combination, then the RAS server will negotiate with the client until it finds an authentication method that will work. Also, there is an option to enable clients to connect without negotiating any form of authentication, which is *Allow remote PPP clients to connect without negotiating any authentication method*.

The Encryption tab contains four data encryption options. The data encryption options specify the types of data encryption, which include IPSec and **Microsoft Point-to-Point Encryption** (**MPPE**). IPSec is described in Chapter 4, and MPPE is a starting-to-ending-point encryption technique that uses special encryption keys varying in length from 40 to 128 bits. As is true for authentication protocols, you can select to use one or a combination of encryption options to match what the client is using. The encryption options are:

- *No Encryption:* Enables clients to connect and not employ data encryption
- *Basic:* Enables clients using 40-bit encryption key MPPE (available in Windows operating systems sold throughout the world) or IPSec
- *Strong:* Enables clients using 56-bit encryption key MPPE or IPSec

Expect Microsoft to soon include a "strongest" option for 128-bit encryption using MPPE via an upgrade or service pack.

IPSec requires that you first configure IPSec as a TCP/IP property on the RAS server (using the Network Dial-up and Connections tool, see Chapters 4 and 6). MPPE requires that the client have MS-CHAP, MS-CHAP v2, or EAP authentication support. Also, if only No Encryption is checked, then encryption is not used with any client, regardless of the client's capabilities.

Table 12-3 Dial-in and VPN Remote Access Policies Tabs

Tab	Description
Advanced	Used to designate connection attributes, such as RADIUS, frame types, AppleTalk zones, special filters, and many others
Authentication	Used to select the type or types of authentication methods, such as EAP, CHAP, MS-CHAP, MS-CHAP v2, PAP, and SPAP (or no authentication)
Dial-in Constraints	Used to set dial-in limitations, such as times of the day and days of the week when the RAS servers can be accessed, amount of time a connection can be idle before it is disconnected, maximum session time, dial-in number, and media through which to dial in (such as ISDN, X.25, modem, and fax)
Encryption	Used to designate encryption levels: no encryption, basic, strong
IP	Used to define how TCP/IP dial-in clients obtain an IP address—for example, by using the server user account settings—and to set up packet filters to limit which IP addresses can access the RAS servers
Multilink	Used to enable Multilink connections, when RAS is set up for Multilink, and to specify Multilink BAP settings

Configuring a Dial-up Connection for a RAS Server

After RAS is installed and configured, create one or more ways for the RAS server to connect to the network so it can be accessed by clients. Besides the Local Area Connection that you set up when installing Windows 2000 Server, you can also create other connections to match your particular connectivity needs, by configuring a dial-up connection to a private network or ISP through a phone line, for example, or by enabling clients to connect through a telecommunications line or the Internet. You create any of these connections by opening the Network and Dial-up Connections tool. For example, if you want to connect through a modem and dial-up telephone line:

1. Open the Network and Dial-up Connections tool.
2. Double-click Make New Connection, and click Next.
3. Click Dial-up to private network (see Figure 12-13), and click Next.

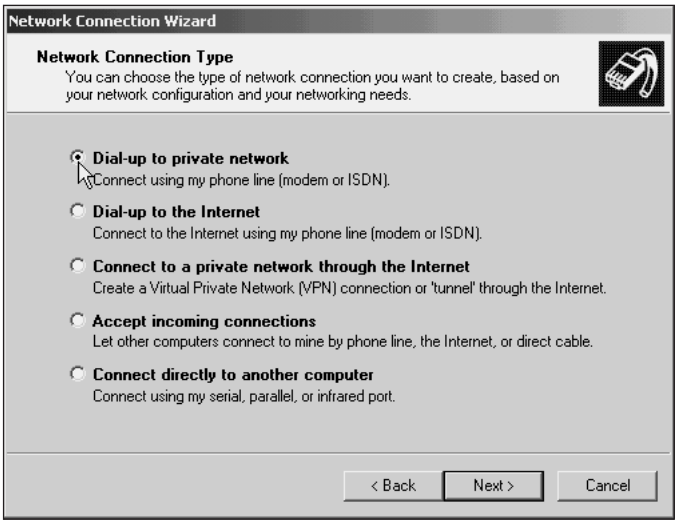

Figure 12-13 Creating a new connection

4. Enter the telephone number of the private network to which to connect, and click Next.
5. Click *For all users* so that other users can connect through this connection, and click Next.
6. If this is a small office and several users connect through a server connected to the Internet, click *Enable Internet Connection Sharing for this connection*, and click Next. Click Yes to the warning about changing the IP address, if you selected to use Internet connection sharing. Click Next.
7. Enter a name for the connection and click Finish.

Configuring Clients to Connect to RAS through Dial-up Access

Common RAS clients include Windows 95, 98, NT, and 2000. You have already learned how to install RAS in Windows 2000 and to set up a dial-up connection. To access a RAS server from the other operating systems, you must also install RAS and configure a dial-up connection on those clients. Hands-on Project 12-7 gives you practice installing RAS in Windows NT 4.0. To install RAS and dial-up connectivity in Windows 95 or 98, use the following general three-stage process:

1. Install the dial-up networking software.
   a. Open the Control Panel.
   b. Double-click the Add/Remove Programs icon.
   c. Click the Windows Setup tab.
   d. Click the Communications box and then the Details button.

e. Click the Dial-up Networking box and click OK.

f. Click OK.

g. If requested, insert the Windows 95 or 98 CD-ROM and provide the drive and path to the operating system files.

h. Click OK when the installation is completed, and if requested, click Yes to reboot.

2. Create and configure the dial-up networking connection:

a. Double-click My Computer.

b. Double-click the Dial-up Networking folder. If the Make New Connection Wizard does not start automatically, double-click the Make New Connection icon.

c. The wizard will detect the modem installed at the workstation.

d. Check the modem information to verify that it is correct. Enter a name to identify the dial-up connection (in the *Type a name for the computer you are dialing* box), and click Next.

e. Enter the area code, telephone number, and country code of the RAS server, and click Next.

f. Click Finish.

g. An icon for the dial-up connection is created in the Dial-up Networking folder in My Computer; open the Dial-up Networking folder.

h. Right-click the newly created icon, and click Properties.

i. Click the Server Type button in Windows 95 (early version) or the Server Types tab in the later version of Windows 95 and in Windows 98.

j. Specify PPP as the protocol for the dial-up server.

k. Click the appropriate Advanced options, such as "Log on to network".

l. Select the appropriate protocol, such as TCP/IP.

m. Click the TCP/IP Settings button and enter the appropriate IP addresses for the workstation and the RAS server.

n. Click OK three times in the early version of Windows 95 or twice in the later version of Windows 95 or in Windows 98 to save your changes.

3. Establish networking settings.

a. Open the Control Panel and double-click the Network icon.

b. Click the Configuration tab, highlight Dial-up Adapter, and click the Properties button.

c. On the Driver Type tab, select Enhanced mode (32-bit or 16-bit) NDIS driver.

d. Click the Bindings tab and checkmark the desired protocol, such as TCP/IP.

e. In the Advanced tab, select the appropriate properties, and click OK to return to the Configuration tab.

f. Select each protocol associated with the dial-up adapter (one at a time), such as TCP/IP –> Dial-up Adapter, and click Properties.

g. Check to make sure the properties match the need for the dial-up service.

h. If TCP/IP –> Dial-Up Adapter is used, make sure the necessary IP address information is provided for its properties.

i. Click OK when you are finished entering the properties.

j. Click OK in the Network dialog box. Insert the installation CD-ROM; if requested, and also restart the computer, if requested.

CONFIGURING A VPN

A Windows 2000 server can be configured as a VPN server for access through the Internet, through routers, and through telecommunications lines, such as frame relay. The general steps for setting up a VPN server are as follows:

1. Create a network connection to an ISP, a public network, or a private network by installing a WAN adapter in the server, such as an ISDN TA, or by connecting through an access server or router that goes to a WAN connection. Set up WAN access addressing as instructed by your WAN or Internet service provider.
2. Install the Routing and Remote Access Service and configure it as a virtual private network (VPN) server.
3. Establish the remote access policies and profile, including setting up EAP authentication.
4. Configure the number of PPTP and L2TP ports.

Creating a Network Connection to the ISP

The specific methods for configuring the connection to the WAN will vary, depending on whether you use a WAN adapter, an access server, or a router to connect. For example, the general steps if you are using a WAN adapter are as follows (each step may vary, depending on the equipment and manufacturer):

1. Begin by installing the WAN adapter in an appropriate expansion slot in the server.
2. Use the Add/Remove Hardware Wizard to configure the WAN adapter (see Chapter 6).
3. Use the Network and Dial-up Connections tool to create a connection to the WAN network, as described in the section "Configuring a Dial-up Connection for a RAS Server."
4. Use the Network and Dial-up Connections tool to configure Internet and local area network connections for TCP/IP according to your ISP's instructions (to configure the IP address and subnet mask, see Chapter 6).

If you are using an access server, follow these general steps (which may vary depending on the manufacturer's specific instructions):

1. Use the Network and Dial-up Connections tool to create a VPN connection to an access server or a router, as described in the section "Configuring a Dial-up Connection for a RAS Server."
2. Use the Network and Dial-up Connections tool to configure the VPN and local area network connections for TCP/IP according to your ISP's instructions (to configure the IP address and subnet mask, see Chapter 6).

Installing a VPN Server

To install and configure a VPN server, begin by opening the Routing and Remote Access tool as an MMC snap-in or from the Administrative Tools menu, by clicking Start, pointing to Programs, pointing to Administrative Tools, and clicking Routing and Remote Access. Then:

1. Click the Action menu and click Add Server.
2. The Add Server dialog box enables you to install routing and VPN capabilities on the local server or on another Windows 2000 server connected to the network or in the domain. For example, click *This computer* to install routing and VPN on the local server, and then click OK.

Before you select a server, keep in mind that routing and remote access services, such as RAS, should not already be set up on that server if you want to perform a fresh installation.

3. Under the tree, right-click the computer and click Configure and Enable Routing and Remote Access.
4. Click Next after the Routing and Remote Access Server Setup Wizard starts.
5. Click *Virtual private network (VPN) server* and click Next.
6. The protocols that are already installed on the server are displayed. Click Yes to use all of the protocols listed, or click No if you need to add protocols to the list to support through the VPN server. Click Next. If you clicked No, click Next and then click Finish on the next screen to end the Wizard, install the additional protocols, and restart the Wizard.
7. If you clicked Yes and AppleTalk is among the supported protocols, the Wizard displays a dialog box to enable AppleTalk clients to access the VPN server through the Guest account. Decide whether to enable AppleTalk access, and click Next.
8. Select the method to access the WAN network or the Internet. For example, if access is through a WAN adapter, click that adapter in the Internet connection box, and then click Next.

9. Decide whether to use DHCP or IP address assignment or to assign a static range of addresses. For example, if you decide to assign a static range, click *From a specified range of addresses* as the means to assign IP addresses, and click Next. Click the New button and then enter the range of IP addresses that can be used (see Figure 12-14). Click OK and click Next. If you choose to use DHCP instead of a static range, configure the DHCP Relay Agent, as already described in the section "Configuring a DHCP Agent" (but click the new VPN server instead of a RAS server).

Keep in mind that the upper limit of addresses that can be assigned to a static pool is 253.

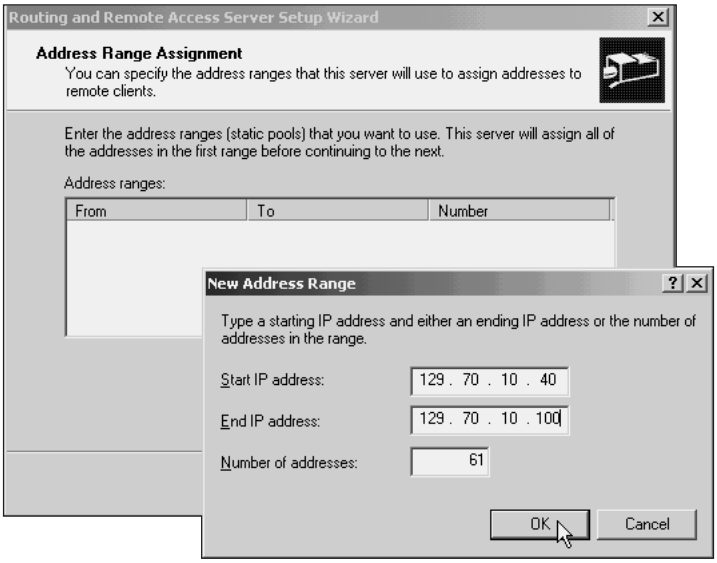

Figure 12-14 Providing a range of addresses for a VPN server

10. Specify whether this will be a RADIUS server, and click Next.
11. Click Finish.

Configuring VPN Server Properties, a VPN Policy, and a VPN Profile

You can further configure a VPN server in the same way as for RAS, by configuring its properties, remote access policies, and profile. After the VPN server installation is complete, right-click the server in the tree and click Properties to configure the server properties. Make certain that the VPN server is configured as a router (see Figure 12-8) by checkmarking the Router box and then clicking *LAN and demand-dial routing*. The other tabs in the Properties dialog box enable you to modify the configuration, for example by using the IP tab to add or remove

static IP addresses from the address pool. If you are using Multilink, configure the Multilink connectivity by clicking the PPP tab (refer to Figure 12-9).

After you examine and configure the VPN server properties, set up the remote access policies and profile. If you are managing multiple VPN and RAS servers, install a RADIUS server and install IAS, as previously explained in this chapter. Set the remote access policies and profile in IAS. If there is only one VPN server, double-click the server to display the objects in the tree under it (if they are not already displayed). Next, click *Remote Access Policies* under the server, and double-click *Allow access if dial-in permission is enabled* to view the policy settings (see Figure 12-11). The remote policy settings are identical to those already discussed for a RAS server. Make sure that either *Grant remote access permission* or *Deny remote access permission* is selected to match, the conditions you establish, such as the day and time access to the VPN server.

As previously described for managing RAS and VPN access, consider controlling access by creating groups and granting group access by clicking the Add button on the screen shown in Figure 12-11 and clicking Windows-Groups to select the group or groups to have access.

Edit the remote access profile by clicking the Edit Profile button in the *Allow access if dial-in permission is enabled* Properties dialog box (refer to Figure 12-11). The profile options are nearly identical to those that apply to a RAS server (refer to Figure 12-12). Make sure that the EAP box is checked when you configure security, because many users will access the VPN server through routers.

Also, click the Encryption tab and set the types of encryption, which include No Encryption, Basic, and Strong. Click the Multilink tab if you are set up to use Multilink, which enables you to configure the same Multilink and BAP settings already described for a RAS server.

Configure the Number of Ports

Consult with your WAN provider on the number of ports that are available through your WAN connection. Once you have this information, configure the number of WAN ports in the VPN server. To configure the number of ports, right-click Ports in the tree under the server and click Properties. Double-click WAN Miniport (PPTP) and set the appropriate number of ports (see Figure 12-15). Also, double-click WAN Miniport (L2TP) and configure the same number of ports.

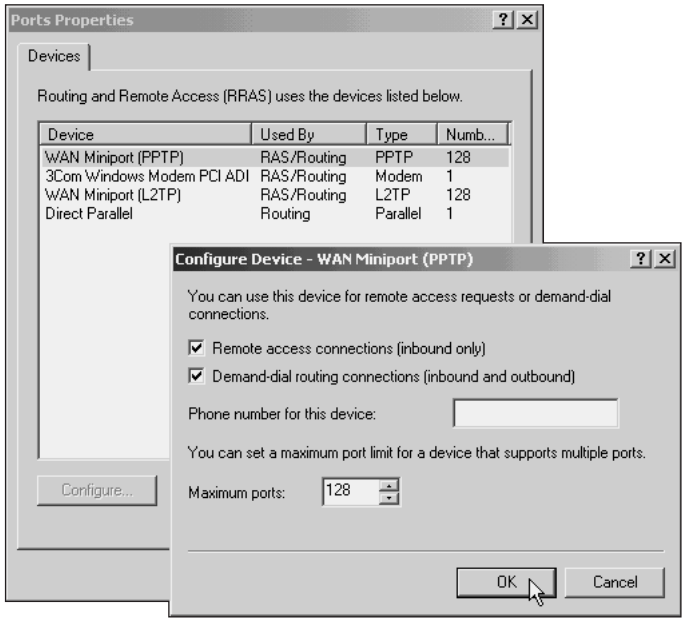

Figure 12-15 Configuring the number of ports

TROUBLESHOOTING RAS AND VPN INSTALLATIONS

12

Troubleshooting a RAS or VPN server communications problem can be divided into hardware and software troubleshooting tips.

Hardware Solutions

If no one can connect to the RAS or VPN server, try these hardware solutions:

- Use the Add/Remove Hardware tool or Device Manager to make sure modems and WAN adapters are working properly. Also, use the Device Manager to make sure that a modem or WAN adapter has no resource conflicts. If there is a conflict, fix it immediately.
- Use the Network and Dial-up Connections tool to test modem dial-up connections and VPN WAN connections. To test a connection, open the tool and click the connection you want to test.
- If you are using an access server, make sure it is properly connected to the network and to the telecommunications and WAN lines. Also, make sure it has power.
- If you are using one or more internal or external modems connected to the server, make sure the telephone line(s) is (are) connected to the modem(s) and to the wall outlet(s).

- For external modems, make sure the modem cable is properly attached, that you are using the right kind of cable (do not use a null modem cable), and that the modem has power.
- For internal modems, make sure they have a good connection inside the computer. Reseat internal modem cards, if necessary.
- Test the telephone wall connection and cable by temporarily attaching a telephone to the cable instead of the modem and making a call.

Software Solutions

Try the following software solutions if no one can access the RAS or VPN server:

- Use the Computer Management tool to make sure the Remote Access Auto Connection Manager and the Remote Access Connection Manager services are started.
- Make sure that a RAS or VPN server is enabled. To check, right-click the server in the Routing and Remote Access tool and make sure that the Remote Access Server box is checkmarked on the General tab (for a RAS or VPN server).
- Use the Ports option under the RAS or VPN server name to check the status of configured ports. Check to determine if all ports are being used. Double-click a port to view its connection statistics and information, if you think there might be a problem with a specific port.
- If TCP/IP connectivity is used, make sure that the IP parameters are correctly configured, for providing an address pool for a VPN server, for example. If IP configuration depends on DHCP, make sure that the DHCP server is working on the network and that you have configured a DHCP Relay Agent (with the correct hop-count threshold).
- If you are using a RADIUS server, make sure that it is connected and working properly and that IAS is installed.
- If you have configured a remote access policy, check to be sure that it is consistent with the users' access needs. For example, users may not be able to access a RAS or VPN server because the server is set to prevent access at certain times, or because certain users are not in a group that has access to the server.

If only certain clients but not all are having connection problems, try these solutions:

- Check the dial-up networking setup on the clients.
- Make sure the clients are using the same communications protocol as the server, for example PPP, and that they are using an authentication and encryption method that is supported by the RAS or VPN server.
- Make sure that each client has a server account and that each knows the correct account name and password. Also, make sure that accounts have the necessary rights and permissions to access files and folders on the server.

- If you manage access to a RAS or VPN server by using groups, make sure that each user account that needs access is in the appropriate group.
- Make sure the client accounts have been granted dial-up access capability and have the correct callback setup.
- For a dial-up RAS connection, determine if the clients' modems are compatible with the modems on the RAS server.

Monitoring User Connections

A monitoring capability is available to view user accounts that are in session on a RAS or VPN server. Monitoring connections can help you to develop an understanding of the average user load and aid in diagnosing problems. For example, a common problem on popular RAS servers, particularly in college and university settings, is that some users cannot connect because all ports are frequently busy, indicating that you may need to add more connectivity or another server. Also, you can use the tool to diagnose telephone or communications line problems in situations in which a certain port is never active. To access the tool, open the Routing and Remote Access tool, click the RAS or VPN server under the tree to view its child objects, and then click Remote Access Client(s). The right pane enables you to view the names of users who are connected, the duration of each connection, and the number of ports used by each connection.

Chapter Summary

- A Windows 2000 server configured for RAS enables clients to remotely dial in to a server or a network of servers. Similarly, a Windows 2000 server configured as a VPN server enables clients to remotely access a private network that works like a members-only tunnel through a larger network. VPNs provide added security for remote communications and increase performance through router-based networks.
- Remote access to a Windows 2000 server network can be through regular dial-up telephone lines, special high-speed lines, Internet connections, and routers. Remote traffic over telephone lines is transported through the Point-to-Point Protocol (PPP). Traffic through the Internet or through a VPN is transported via the Point-to-Point Tunneling Protocol (PPTP) and the Layer Two Transport Protocol (L2TP).
- When you set up a RAS or VPN you can manage one or multiple servers through remote access policies and profiles. Creating a RADIUS server and implementing IAS enable you to manage two or more RAS and VPN servers through coordinated remote access policies. Remote access policies and profiles are used to establish how a server is available to users and to set up security.

In the next chapter, you learn more about network interoperability, for example setting up a Web server, connecting to a Novell NetWare server, and setting up terminal services. You also learn more about Windows 2000 DCHP and DNS.

KEY TERMS

access server — A device that connects several different types of communications devices and telecommunication lines to a network, providing network routing for these types of communications.

aggregate link — Linking two or more communications channels, such as ISDN channels, so that they appear as one channel, but with the combined speed of all channels in the aggregate.

Bandwidth Allocation Control Protocol (**BACP**) — Similar to BAP, but is able to select a preferred client when two or more clients vie for the same bandwidth.

Bandwidth Allocation Protocol (**BAP**) — A protocol that works with Multilink in Windows 2000 Server to enable the bandwidth or speed of a remote connection to be allocated on the basis of the needs of an application, with the maximum allocation equal to the maximum speed of all channels aggregated via Multilink.

bits per second (**bps**) — Number of binary bits (0s or 1s) sent in one second, a measure used to gauge network, modem, and telecommunications speeds.

Challenge Handshake Authentication Protocol (**CHAP**) — An encrypted handshake protocol designed for standard IP- or PPP-based exchange of passwords. It provides a reasonably secure, standard, cross-platform method for sender and receiver to negotiate a connection.

CHAP with Microsoft extensions (**MS-CHAP**) — A Microsoft-enhanced version of CHAP that can negotiate encryption levels and that uses the highly secure RSA RC4 encryption algorithm to encrypt communications between client and host.

CHAP with Microsoft extensions version 2 (**MS-CHAP v2**) — An enhancement of MS-CHAP that provides better authentication and data encryption and that is especially well suited for VPNs.

data communications equipment (**DCE**) — A device that converts data from a DTE, such as a computer, to be transmitted over a telecommunications line.

data terminal equipment (**DTE**) — A computer or computing device that prepares data to be transmitted over a telecommunications line to which it attaches by using a DCE, such as a modem.

DHCP Relay Agent — A server, such as a RAS or VPN server, or computer that broadcasts IP configuration information between the DHCP server on a network and the client acquiring an address.

digital subscriber line (**DSL**) — A technology that uses advanced modulation technologies on regular telephone lines for high-speed networking at speeds of up to 60 Mbps between subscribers and a telecommunications company.

Extensible Authentication Protocol (**EAP**) — An authentication protocol employed by network clients that use special security devices such as smart cards, token cards, and others that use certificate authentication.

frame relay — A WAN communications technology that relies on packet switching and virtual connection techniques to transmit at from 56 Kbps to 45 Mbps.

Integrated Services Digital Network (**ISDN**) — A telecommunications standard for delivering data services over digital telephone lines with a current practical limit of 1.536 Mbps and a theoretical limit of 622 Mbps.

Internet Authentication Service (**IAS**) — Used to establish and maintain security for RAS, Internet, and VPN dial-in access, and can be employed with RADIUS. IAS can use certificates to authenticate client access.

Layer Two Tunneling Protocol (**L2TP**) — A protocol that transports PPP over a VPN, an intranet, or the Internet. L2TP works similarly to PPTP, but unlike PPTP, L2TP uses an additional network communications standard, called Layer Two Forwarding, that enables forwarding on the basis of MAC addressing.

line device — A DCE, such as a modem or ISDN adapter, that connects to a telecommunications line.

Microsoft Point-to-Point Encryption (**MPPE**) — A starting-to-ending-point encryption technique that uses special encryption keys varying in length from 40 to 128 bits.

modem — A modulator/demodulator that converts a transmitted digital signal to an analog signal for a telephone line. It also converts a received analog signal to a digital signal for use by a computer.

Multilink or **Multilink PPP** — A capability of RAS to aggregate multiple data streams into one logical network connection for the purpose of using more than one modem, ISDN channel, or other communications line in a single logical connection.

Password Authentication Protocol (**PAP**) — A nonencrypted plaintext password authentication protocol. This represents the lowest level of security for exchanging passwords via PPP or TCP/IP. Shiva PAP (SPAP) is a version that is used for authenticating remote access devices and network equipment manufactured by Shiva (now part of Intel Corporation).

Point-to-Point Protocol (**PPP**) — A widely used remote communications protocol that supports IPX/SPX, NetBEUI, and TCP/IP for point-to-point communication (for example, between a remote PC and a Windows 2000 server on a network).

Point-to-Point Tunneling Protocol (**PPTP**) — A remote communications protocol that enables connectivity to a network through the Internet and connectivity through intranets and VPNs.

Remote Access Services (**RAS**) — Microsoft software services that enable off-site workstations to access a Windows 2000 server through telecommunications lines, the Internet, or intranets.

Remote Authentication Dial-In User Service (**RADIUS**) — A protocol and service set up on one RAS or VPN server, for example in a domain, when there are multiple RAS or VPN servers to coordinate authentication and to keep track of remote dial-in statistics for all RAS and VPN servers.

Serial Line Internet Protocol (**SLIP**) — An older remote communications protocol that is used by UNIX computers. The modern compressed SLIP (CSLIP) version uses header compression to reduce communications overhead.

Shiva Password Authentication Protocol (**SPAP**) — See Password Authentication Protocol.

T-carrier — A dedicated leased telephone line that can be used for data communications over multiple channels for speeds of up to 44.736 Mbps.

Telephone Application Programming Interface (**TAPI**) — An interface for communications line devices (such as modems) that provides line device functions, such as call holding, call receiving, call hang-up, and call forwarding.

terminal adapter (**TA**) — Popularly called a digital modem, links a computer or a fax to an ISDN line.

Universal Modem Driver — A modem driver standard used on recently developed modems.

virtual private network (**VPN**) — A private network that is like a tunnel through a larger network—such as the Internet, an enterprise network, or both—that is restricted to designated member clients only.

X.25 — An older packet-switching protocol for connecting remote networks at speeds up to 2.048 Mbps.

Review Questions

1. One of your users is trying to connect to a RAS server, but is not able to make the connection. All ports and communications devices at the server end are working. The user, who is running Windows NT 4.0 Workstation, has checked his modem and telephone system, and all are working. Which of the following might be the problem?
   a. The user's modem has a top speed of 33.3 Kbps, and the RAS server modem cannot step down from 56 Kbps.
   b. The user's account is denied dial-in access in the account's properties.
   c. The user's dial-up connectivity is set to use SLIP:Internet.
   d. all of the above
   e. only a and b
   f. only b and c
2. You have installed a RAS server to obtain IP addresses from a DHCP server that is connected to the network. No error messages were displayed during the installation, but for some reason, IP addresses are not being automatically assigned to RAS clients. What step might you have omitted?
   a. configuring a DHCP relay agent
   b. configuring a "hard-coded" IP address at each client
   c. disabling IPX, which creates routing problems with TCP/IP
   d. all of the above
   e. only a and b
   f. only b and c

3. Your assistant set up RAS to use AppleTalk. Now it seems that all kinds of users have figured out how to access a wide range of network resources without having an account. What would you check first?
   a. that AppleTalk is only enabled for zone 1
   b. that the DHCP server is online
   c. that the Guest account's rights and permissions security are carefully limited
   d. that the DNS server is properly communicating with the DHCP server
4. You are converting a RAS server that runs Windows NT Server 4.0 to Windows 2000 Server. The server you are converting is set up to use SLIP. Which of the following steps should you complete when upgrading the RAS server to Windows 2000 Server?
   a. Convert to use CSLIP as the remote communications protocol and make sure clients are also set up to use CSLIP.
   b. Convert to use PPP as the remote communications protocol and make sure clients are also set up to use PPP.
   c. Replace the modems in the server with ISDN adapters, because Windows 2000 RAS no longer supports asynchronous modem connections.
   d. all of the above
   e. only a and c
   f. only b and c
5. Your network is located in Philadelphia, but five employees in your organization telecommute from a shared office that is in Washington, D.C. Each of the telecommuters has her or his own telephone line and dedicated number. How can you set up security so that the RAS server verifies each user by her or his telephone number?
   a. Set up callback security on each user's account so that only a specific number is called back.
   b. Assign a static IP address to each of the five users and set up a telephone number in the RAS server that is assigned to each IP address.
   c. Control RAS server access through a remote access policy that contains a list of telephone numbers that the server can call back.
   d. You cannot set up verification on the basis of a specific telephone number, only by area code.
6. About half of your RAS server's clients use smart cards. What authentication protocol must you configure for them?
   a. Password Authentication Protocol (PAP)
   b. Extensible Authentication Protocol (EAP)
   c. Shiva Password Authentication Protocol (SPAP)
   d. CHAP with Microsoft extensions (MS-CHAP)

7. When you set up Routing and Remote Access services, which of the following is not an option?
   a. to install a RAS server
   b. to install a VPN server
   c. to install an Internet connection server
   d. to install a telephone switching system for remote callers
8. You have two modems installed in a server for RAS communications. Both are 56 Kbps modems and both telecommunications lines are capable of 56 Kbps communication, but right now users on only one line can transmit at 56 Kbps. Connections to the other line are never over 14.4 Kbps. What should you check to troubleshoot the problem?
   a. Make sure that the port speed on the slower line is set at 56 Kbps or higher.
   b. Check to determine if the slower line has a RAS speed filter set up in the remote access policies.
   c. Connect the modem to the telephone line by using a faster telephone cable.
   d. If a telephone is connected through an output jack to the slower modem, disconnect the cable to the telephone, because it creates extra resistance.
9. How can you best configure authentication for a VPN server?
   a. through a modem's or WAN adapter's properties
   b. by using the CSLIP protocol
   c. by creating remote access policies and a profile
   d. by setting RAS and VPN user access rights through the Active Directory Users and Computers tool
10. Which of the following protocols can be transported by PPP?
    a. NWLink
    b. NetBEUI
    c. TCP/IP
    d. all of the above
    e. only a and c
    f. only b and c
11. Your organization is setting up five VPN servers and wants to establish one set of remote access policies and one place from which to coordinate all of the VPN servers. How is this possible?
    a. Make one of the VPN servers a RADIUS server.
    b. Establish one VPN global group that is enabled to access all of the VPN servers.
    c. Add a RAS server as a lead domain controller.
    d. Each VPN server will automatically coordinate with all other VPN servers.

12. After you set up a VPN server and test it over a WAN link, you see a message that says it is unable to transport via L2TP (Layer Two Tunneling Protocol). What should you check first to diagnose this problem?
    a. Make sure that you have enabled L2TP ports and specified the number of L2TP ports to match the number of ports available over the WAN connection.
    b. Disable PPTP because it is conflicting with L2TP communications.
    c. Make sure that the VPN server is configured to transport NetBEUI as well as TCP/IP, because L2TP is a special Microsoft network routing protocol.
    d. This message is normal because you have set up a T-1 WAN link, and T-1 does not enable use of L2TP.
13. You want to set up a RAS server that enables users to dial in through a group of 12 modems or through an ISDN line. What might you use in addition to the RAS server to provide these dial-in links?
    a. a bridge
    b. an access server
    c. a port expander
    d. several dedicated computers that have free expansion slots
14. You need to take your VPN server offline for some maintenance. Is there a way that you can disable access to the server for a short time?
    a. Use the remote access policies to change the hours that the server is available, so that it cannot be accessed when you want it offline.
    b. Remove the check mark in the Remote access server box in the server's properties for the time that you want to make the server unavailable.
    c. Use the *Disconnect users from network* feature in the server's properties for the time that you want to make the server unavailable.
    d. all of the above
    e. only a and b
    f. only b and c
15. The computer committee at your business has been discussing setting up a VPN that includes remote access through high-speed communications lines. The committee has already contacted the local telephone company and found that they can connect using T-1, T-3, and frame relay. Also, they have found that they can connect remote networks using any of these links attached to routers. Which of these is compatible with a Windows 2000 VPN server?
    a. T-1 and T-3 are compatible, but frame relay and routers are not.
    b. T-3 and frame relay are compatible, but T-1 and routers are not.
    c. Only frame relay with routers is compatible.
    d. T-1, T-3, frame relay, and routers all are compatible.
    e. None of the options is compatible, because a VPN server can only connect through an ISDN line.

16. Your VPN server is configured to enable Multilink as a way to enable the aggregation of frame relay channels when users need more bandwidth—for example, for multimedia applications. However, when a user connects, the server does not seem to adjust for the amount of bandwidth needed by a user. How can you fix the problem?
    a. Restrict Multilink to increments to 56 Kbps per port.
    b. Configure the VPN server to limit the maximum number of ports to 1.
    c. Configure the VPN server to dynamically use the Bandwidth Allocation Protocol (BAP) along with Multilink.
    d. all of the above
    e. only a and c
    f. only a and b
17. You have set up a VPN server to connect to another network through a router. The server handles incoming traffic through the router properly, but does not seem to reliably route outgoing traffic. Where might you look to solve this problem?
    a. Make sure that no internal routing interfaces are configured.
    b. Make sure that the VPN server is enabled as a router.
    c. Enable the VPN server to double as a RAS server, because RAS servers are able to route.
    d. Set up the VPN server to use the Layer 4 routing protocol.
18. What tool(s) can be used to help you diagnose a resource conflict between a WAN adapter and another device in a RAS or VPN server?
    a. Device Manager
    b. Routing and Remote Access tool
    c. Active Directory Domains and Trusts tool
    d. all of the above
    e. only a and c
    f. only b and c
19. You have set up a VPN server so that remote clients can access Windows 2000 servers on a network that uses only TCP/IP and on which the VPN connection is through the Internet. When a client accesses that VPN server from home by connecting through an Internet connection, what protocol(s) is that client using?
    a. TCP/IP
    b. PPTP
    c. PPP
    d. all of the above
    e. only a and c
    f. only b and c

20. Which of the following tools enables you to monitor client connections to a RAS or VPN server?
    a. Active Directory Users and Computers tool
    b. Routing and Remote Access tool
    c. Security MMC snap-in
    d. IP Routing tool
21. All of your RAS server clients are configured to use 56-bit encryption key MPPE, but when you use a network analyzer it appears that none of the communications is actually encrypted. Which of the following might be the problem?
    a. The remote access policies profile is set only for *No Encryption* and should instead be set for *Strong*.
    b. The remote access policies profile must be set for *Basic* encryption.
    c. The RAS server is not set up to use EAP authentication.
    d. Multilink must be configured in order for clients to use 128-bit encryption key MPPE.
22. You are planning to connect your RAS server to an ISDN line. What type of line device or adapter must you purchase for the server?
    a. asynchronous modem
    b. X.25 adapter
    c. terminal adapter
    d. synchronous modem
23. On your TCP/IP network, each VPN client must go through two routers to reach the VPN server, and the VPN server must go through one router to communicate with a DHCP server. If the VPN server is set up to use DHCP, what should the hop-count threshold be when you configure the DHCP Relay Agent at the VPN server? (Remember that a VPN server is also configured as a router.)
    a. 1
    b. 2
    c. 3
    d. 4
24. Which of the following can be Windows 2000 RAS server clients?
    a. Windows NT 3.51
    b. Windows 95
    c. Windows 3.11
    d. all of the above
    e. none of the above
    f. only a and b

25. You have set up a RAS server that is to be accessed by clients running Windows 2000 Professional and a few clients still running MS-DOS. What authentication should you configure for the RAS server?
    a. Password Authentication Protocol (PAP)
    b. Challenge Handshake Authentication Protocol (CHAP)
    c. CHAP with Microsoft extensions version 2 (MS-CHAP v2)
    d. all of the above
    e. only a and b
    f. only a and c

HANDS-ON PROJECTS

Project 12-1

In this project you practice optimizing RAS communications by making sure that the speed set for a serial communications port matches the capabilities of a modem connected to that port on a RAS server. Assume that the modem can transmit at 56 Kbps. You also practice using the Hardware Troubleshooter, in case there is a connection problem. You will need a computer running Windows 2000 Server or Windows 2000 Professional, with a modem installed.

To check the serial port's setup and use the Hardware Troubleshooter:

1. Click **Start**, point to **Programs**, point to **Administrative Tools,** and click **Computer Management**.
2. Click **Device Manager** in the tree.
3. Double-click **Modems** in the right pane, and then double-click the modem attached to the computer, for example **3Com Windows Modem PCI ADI**.
4. Click the **General** tab, if necessary. Is the modem working properly? Record your findings in your lab journal or in a word-processed document.
5. Click the **Troubleshooter** button to view how to access troubleshooting advice for situations in which the modem and port are not working. Record which of the options address modem problems. How would you solve a situation in which the modem is not detected? Close the Hardware Troubleshooter.
6. Click the **Modem** tab. To what port is the modem attached? What is the setting for the Maximum Port Speed?
7. If the Maximum Port Speed is less than 56 Kbps, change it by clicking the list arrow and selecting **57600** or **115200**.
8. Click the **Advanced** tab and click the **Change Default Preferences** button.
9. How can you use this button to change parameters such as data bits, parity, stop bits, and enabling data compression? Record how you might use these capabilities to resolve problems in which users' modems fail to communicate with the modem in the server.

10. Click **Cancel**.
11. Click **OK** and then close the Computer Management tool.

The tabs and options associated with a particular modem can vary, depending on the modem driver. Examine all of the tabs and use the appropriate options for your particular modem.

Project 12-2

In this project, you practice installing RAS to make a Windows 2000 Server a RAS server. The Windows 2000 server that you use might not already be set up as a RAS or VPN server. If it is, open the Routing and Access tool as described in Step 1, right-click the server under the tree, and click Delete to remove it.

To install RAS:

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and click **Routing and Remote Access**.
2. Right-click **Routing and Remote Access** in the tree and then **Add Server**.
3. Click **This computer**, if necessary. How would you install RAS on another network server or another server in a domain? Record your observations. Click OK.
4. In the left-pane tree, right-click the computer and then click **Configure and Enable Routing and Remote Access**.
5. Click **Next**.
6. What options can be installed through this wizard? Record your observations.
7. Click **Remote access server** and click **Next**.
8. What protocols are displayed? How would you add a protocol that is not on the list? Click **Yes** and then click **Next**.
9. If AppleTalk is installed, checkmark the box to enable AppleTalk clients to access the Guest account. What precautions should you take in this situation?
10. If TCP/IP is installed, click **Automatically** in the IP Address Assignment dialog box, if necessary. What is the other option, and what would happen if you specified that option? Click **Next**.
11. Click **No**, if necessary, so that this server is not set up as a RADIUS server and then click Next. What is the advantage of using a RADIUS server? What additional service should you set up for security management?
12. Click **Finish**. What message is displayed, if you specified use of DHCP? Click **Yes** if you see an informational message. Leave the Routing and Remote Access tool open for the next project.

Project 12-3

Because you set up RAS to use DHCP in Hands-on Project 12-2, you now need to set up a DHCP Relay Agent.

To set up a DHCP Relay Agent:

1. Make sure the Routing and Remote Access tool is open, and if not, open it.
2. Double-click the RAS server in the tree, for example **Lawyer**, if the child objects are not already displayed under it.
3. What child objects are displayed in the tree under the RAS server? Click each object to quickly review what it does, and record your observations in your lab journal or in a word-processed document.
4. Click **IP Routing** in the tree, if necessary, to view objects under it.
5. Click **General**, if necessary, under IP Routing in the tree. How would you determine the IP address of the local connection for the RAS server?
6. Right-click **DHCP Relay Agent** under IP Routing in the tree, and click **Properties**.
7. Enter the IP address of the RAS server, for example **129.70.10.1**, and click **Add**.
8. Click **OK**.
9. Click **DHCP Relay Agent** under IP Routing in the tree, and then double-click the interface, such as **Internal**, in the right pane. How would you set the hop-count threshold? Click **Cancel**. Leave the Routing and Remote Access tool open for the next project.

Project 12-4

Assume that you are using a T-3 connection to a RAS or VPN server and you want the ability to enable clients to use Multilink. This project enables you to view where to set up Multilink.

To view the Multilink configuration options:

1. Right-click the RAS server that you created in Hands-on Project 12-2, and click **Properties**.
2. What tabs are displayed? Click each tab and record your general observations of its purpose.
3. Click the **PPP** tab.
4. What options are available for configuring Multilink? Which option would you check to enable use of callback security?
5. Click **Cancel**. Leave the Routing and Remote Access tool open.

Project 12-5

In this activity, you practice setting dial-in security on a user's account. Before you begin, create a practice account or use an account that is specified by your instructor. (This project assumes that the Active Directory is installed.)

To set dial-in security:

1. Open the Active Directory Users and Computers tool, and double-click the domain to display the child objects under it in the tree.
2. Click the container in which the account is located, such as **Users**.
3. Double-click the account you created or that is specified by your instructor.
4. Click the **Dial-in** tab (depending on the resolution of your monitor, you may need to click the right arrow to view the tab before you can click it).
5. Click **Control access through Remote Access Policy** (or if it is deactivated because you are in mixed mode, click a different option). What other options are available for remote access permission?
6. Click **Set by Caller (Routing and Remote Access Service only)**.
7. How would you assign a static IP address for a client that dials in remotely?
8. Click **OK** and then close the Active Directory Users and Computers tool.

Project 12-6

In this project, you set up remote access policies and edit the profile of the RAS server you created in Hands-on Project 12-2.

To set up the remote access policies and edit the profile:

1. Make sure the Routing and Remote Access tool is open, and if it is not, open it.
2. Double-click the RAS server in the tree, for example **Lawyer**, if necessary to display the child objects under the server.
3. Click **Remote Access Policies** in the tree.
4. Double-click **Allow access if dial-in permission is enabled** in the right pane.
5. Double-click the **Day-And-Time Restrictions matches** parameter in the *Specify conditions to match* box.
6. Drag the pointer to select all of the times of day boxes in the row for Sunday (the top row), and click **Denied**. What happens to the boxes?
7. Drag the pointer to select all of the times of day boxes in the row for Saturday (the bottom row), and click **Denied**.
8. Click **OK**.
9. Check the **Grant remote access permission** radio button.
10. Click the **Edit Profile** button.
11. Click the **Authentication** tab. What protocols are selected by default? Record your observations. Which protocol would you check to enable the use of smart cards?

12. Click the **Encryption** tab. What selections are already made? Record your observations. Also, make sure that **No Encryption**, **Basic**, and **Strong** are all check marked, and if not, check them.
13. Click the **Dial-in Constraints** tab. How would you disconnect users who have had no activity for over 15 minutes?
14. Click **OK**. Click **No** if an information box appears to display Help information because you have changed authentication methods.
15. Click **OK**. Close the Routing and Remote Access tool.

If IAS were installed, you could follow nearly the same steps to configure remote access policies for multiple servers.

Project 12-7

In this project, you install RAS in Windows NT Workstation 4.0 so that it can access a RAS server as a client. You will need the Windows NT Workstation CD-ROM, and the computer should already have a modem installed.

To install RAS in Windows NT Workstation 4.0:

1. Log on as Administrator or using an account with Administrator privileges.
2. Click **Start**, point to **Settings**, and click the **Control Panel**
3. Double-click the **Network** icon, and click the **Services** tab. Click **Add**, select the **Remote Access Service**, and click **OK**.
4. Insert the Windows NT Workstation CD-ROM, provide the path to the CD-ROM drive, and click **Continue**. (If the Windows NT Workstation auto run program starts, close its window.) The RAS setup will automatically detect the modem or it will display the Add RAS Device dialog box, from which you can click Install Modem to start the Install New Modem Wizard.
5. In the Remote Access Setup dialog box, highlight the modem and click the **Configure** button. Set the port to **Dial out only** or to **Dial out and Receive calls**. For example, the modem needs to be able to receive calls if the RAS server at work is set up to call back the user as a security measure to ensure that a known user is requesting access.
6. Click **OK** in the Configure Port Usage dialog box, and click **Continue** in the Remote Access Setup dialog box.
7. Click **OK** in each box to enable client access to network servers using specific protocols (depending on which protocols are installed on the RAS server). For example, click OK in the RAS Server TCP/IP Configuration dialog box.
8. Windows NT Workstation should automatically configure bindings for the remote access. If there is no message that it is configuring bindings, click the Bindings tab on the Network dialog box to initiate the Bindings configuration.

9. Click **Close** in the Network dialog box and remove the Windows NT Workstation CD-ROM. Save any open work and click the option to restart the computer.

To set the dial-up configuration:

1. Double-click **My Computer** and then double-click the **Dial-Up Networking** icon.
2. Click **New** in the Dial-Up Networking dialog box.
3. Enter **RAS** as the name for the automated dial-up connection, and click **Next**.
4. Checkmark **Send my plain text password if that's the only way to connect.** The plaintext password is the password for the user's account on the RAS server. Leave the other boxes blank, and click **Next**.
5. Enter the telephone number of the line attached to the computer's modem in the Phone number text box in the Phone number dialog box. Do not click the box for telephony dialing properties, because the line is a basic telephone line and does not require specialized information. Click **Next**.
6. Click **Finish** in the last dialog box to complete the installation wizard.
7. Back in the Dial-up Networking dialog box, select the connection you just made as the Phonebook entry to dial, click the **More** button, and click **Edit entry and modem properties**.
8. Click the **Server** tab and make sure **PPP:Windows NT, Windows 95 Plus, and Internet** is selected in the Dial-up server type box. Click **OK**.
9. Click **Close** in the Dial-up Networking dialog box.

CASE PROJECT

Aspen Consulting Project: Setting Up RAS and VPN Servers

The International Wheat Association is a nonprofit association of wheat growers, researchers, and bakers that provides a wide range of information about growing, processing, and using wheat and wheat-based products. The association is located in Toronto and has member groups throughout the world. One of the International Wheat Association's most popular services is maintaining a database of research information for all members. The database has been on a Windows NT 4.0 RAS server, but the association has hired you to help them convert this vital service to a new Windows 2000 server set up as a RAS server.

1. In your first meeting with those who manage the research database and the association's small IT staff, you are asked to describe the general issues involved in converting the Windows NT RAS server to a Windows 2000 RAS server. Explain the issues involved and begin preparing a planning paper for the conversion.

2. As you are working on your planning paper, you realize that it provides a good opportunity to introduce other planning issues. Include in the paper issues that will affect the use of the RAS server, which are:
   - Remote access protocols
   - IP addressing
   - Remote access policies
   - Authentication
   - Encryption
   - Multilink connectivity
3. The Windows NT RAS server is currently connected to the outside world through two basic-rate interface ISDN adapters. The association's management would like to dramatically increase connectivity so that over 50 remote clients can access the RAS server at one time. Discuss other connectivity options that are available to them through Windows 2000 RAS capabilities.
4. The IT staff of four people wants you to train them in how to manage the RAS server after it is installed. Provide a preliminary training paper that discusses the tools available to them for configuring, managing, monitoring, and troubleshooting the server.
5. The association's research group has received funding from management to set up a VPN server that can be remotely accessed over the Internet by top-level researchers all over the world. Explain any special configuration and setup steps that the IT staff needs to be aware of for the VPN server setup.

Optional Case Projects for Teams

Team Case One

Mark Arnez asks you to form a group to research dedicated RAS and access servers that are available from computer and network vendors. Form a team to use the Internet and any other means to research and describe these devices and their capabilities. Create a document that can be a resource for other consultants.

Team Case Two

Keep your team together, because Mark is now asking you to prepare a document that describes different ways that organizations can use RAS and VPN servers for business, research, and educational purposes.